CONFIDENTIAL

8 NOV 1978

MEMORANDUM FOR: Chairman, Markings Task Force

25X1

FROM: [redacted]
DDA Representative, Markings Task Force

SUBJECT: Control Markings

1. The Markings Task Force has been discussing the discontinuation of the control marking, "Administrative - Internal Use Only." The arguments for doing away with it are substantial:

a. It has been misused a great deal; and

b. The safeguarding sanctions are not clearly defined.

2. I have discussed the use and need of such a marking with a number of people throughout the DDA. There is a need to protect internal Agency information which if released might be misused or be misleading. These papers include:

a. Management options and recommendations; and

b. Administrative planning and procedures.

3. Discussion for the need to have a positive indicator to alert employees that a document contains such information has been lively and interesting. Some of the arguments for and against include:

a. Some people feel if a piece of paper is not marked, employees will/may take it home and discuss the contents freely.

b. Unclassified government information doesn't need to be marked as it is U.S. Government property and all employees should be aware of this and handle all such material as prescribed by regulations and law.

UNCLASSIFIED When Separated From Enclosure

CONFIDENTIAL

c. What about HR [redacted] (attached), "Care and Use of Official Data"? This regulation is under review for revision as the current definition of "Official Data" includes all overt material received by the CIA, including the New York Times, library books, etc. Those reviewing the regulation are having problems coming to grips with the definition. 25X1

4. In order to provide proper control over Agency internal documents, I suggest we do one of two things:

a. Write a proper definition of "Official Data" and get the regulation out to all employees. If a component is concerned they may indicate on a document "Official Data - Internal Use Only;" or

b. Develop a new control marking for documents which

(1) reflect opinion or recommendations for management policy; or

(2) administrative procedures.

5. The first option appeals as HR [redacted] spells out control of information in general. Sanctions are provided whether the information is marked or not. 25X1

6. The second option implies a new marking with a new definition. We suggest "Agency Restricted" as a marking to meet this need. This could be defined as:

> Information prepared by Agency personnel or consultants, such as that pertaining to opinions, recommendations, interpretations, plans or internal procedures, the disclosure of which could prejudice, hinder or deter the Agency from carrying out essential management or administrative functions.

7. The intent is (1) to ensure that such information is only released to the public through authorized channels and (2) to provide an environment conducive to the uninhibited exchange of ideas. Sanctions for the improper use of an unclassified document should follow those for unauthorized release. (There is opposition to giving a control marking

to documents containing national security information. We have been relying on the classification to control these papers. I submit that even after classifications are no longer valid, the internal nature of some of these documents will remain.)

8. In summary, we need at least to provide a positive indicator to control the dissemination of unclassified management information and administrative procedures.

Signed

[redacted] 25X1

Attachment: a/s

cc: DDO/PCS [redacted]
25X1 NFAC/P&PG [redacted]
25X1 DDS&T [redacted]
25X1 OGC [redacted]
DDA/O [redacted]
ISAS/ [redacted]
ISAS/ [redacted]

21. CARE AND USE OF OFFICIAL DATA. All information, classified or unclassified, received, compiled or created by the Central Intelligence Agency (except personal copies of unclassified personnel papers) is official data and is the property of the United States Government.

a. POLICY

(1) All employees are prohibited from using official data for any purpose other than in the performance of their official duties for or on behalf of the Agency. Official data is not to be held in personal files or set aside for personal use or benefit.

(2) Official data is not to be copied or removed from the files of the Agency for release outside the Agency except by those officials authorized through chain of command by the Director of Central Intelligence.

(3) Any employee who is served with a subpoena which may require the disclosure of official data to a court, the Congress, or a committee of the Congress will promptly inform the General Counsel of the serving of the subpoena, the nature of the information sought, and any circumstances which may bear upon the desirability of making available the official data, so that the General Counsel may advise the Director.

(4) When not in use, official data must be kept in storage facilities which have been approved by the Director of Security. Consequently, documents which contain official data are not to be taken home or stored in private residences unless the use of an approved, secure facility has been authorized in advance by the Director of Security.

(5) In addition to the prohibition against unauthorized disclosure of official data outside the Agency, internal disclosure of official data is limited to those employees whose duties require access to it. Employees are not to disclose official data to those who do not need to know it, nor are they to try to obtain official data they do not need to know.

b. RESPONSIBILITIES

(1) Each individual employed by the Central Intelligence Agency is responsible for the secure handling of official data and for protecting it against unauthorized disclosure. Termination of Agency employment will not affect these responsibilities.

(2) The Director of Personnel is to ensure that all personnel processed through headquarters report to the Office of Security to read this regulation and the statutes referred to in subparagraph c below before entering on duty or separating from the Agency. 25X1

25X1 (3) Chiefs of [ ] installations are to ensure that all [ ] personnel not processed through headquarters read this regulation and the statutes referred to in subparagraph c before entering on duty or separating from the Agency.

(4) Any authorized representative of CIA who negotiates with individuals or organizations for services is to ensure that the appropriate statutory provisions are incorporated in the Secrecy Agreement or contract. The incorporation may be by reference where feasible.

a. **STATUTORY REFERENCES.** Sections 793, 794, and 798, Title 18 of United States Code prohibit certain activities with respect to defense information and provide penalties for violation. Section 793 provides generally that persons who lose defense information without reporting such loss, or gather or transmit defense information with the intent or with reason to believe such information will be used to the injury of the United States or to the advantage of any foreign nation are subject to a fine of $10,000 or 10 years imprisonment or both. Section 794 provides generally that persons who communicate or deliver or attempt to communicate or deliver defense information to any foreign government with intent or reason to believe such information will be used to the injury of the United States or to the advantage of a foreign government are subject to imprisonment for not more than 20 years. If this statute is violated during wartime, the punishment is death or imprisonment for not more than 30 years. Both sections 793 and 794 provide like penalties for a conviction of conspiracy to violate either section. Section 798 provides generally that persons who communicate or otherwise make available to an unauthorized person or publisher, or use in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government any classified information relating to cryptography or communications intelligence are subject to a fine of $10,000 or 20 years imprisonment or both.